The Status of the Claims

1. (Currently amended) A network interface unit for communicating data packets over ~~at least~~ one or more non-secure ~~network~~ networks between one or more client devices ~~on at least~~ associated with one or more local area ~~network~~ networks (LAN) and a secure virtual private network (VPN) node, comprising:

~~means for directly connecting to said at least one LAN,~~

~~means for connecting to said at least one non-secure network,~~

means for authenticating ~~at least one of said~~ the one or more client devices ~~seeking to~~ for access **[[**~~said~~**]]** to the secure VPN node~~, thereby establishing at least one authenticated client device~~;

~~a configuration server for sending configuration information to said at least one authenticated client device,~~

a graphical user interface [[GUI]] server for presenting ~~at least one~~ an authentication menu to the one or more ~~at least selected authenticated~~ client devices, wherein, when a first one of the client devices is incompatible with the authentication menu, the authentication means is to authenticate the first client device in response to an authentication of a second one of the client devices via the authentication menu, the second client device being compatible with the authentication menu;

means for receiving ~~at least a first message reflecting selections~~ a selection from ~~said at least one~~ the menu, the selection corresponding to a connection profile associated with a first type of connection; ~~and~~

means for accessing **[[**~~said~~**]]** ~~at least~~ the one or more non-secure ~~network~~ networks using information ~~in said at least a first message~~[[,]] associated with the selection; and

a security server for establishing a secure ~~connection~~ communication over **[[**~~said~~**]]** the non-secure network between **[[**~~said~~**]]** the LAN and ~~said access node~~ the secure VPN node.

2. (Currently amended) The network interface unit of claim 1, ~~wherein said~~ further comprising a configuration server ~~comprises~~ having a memory for storing configuration information for ~~at least one~~ the client ~~device~~ devices, and means for retrieving the configuration information ~~for at least selected ones of said client devices~~ from **[[**~~said~~**]]** the memory ~~upon subsequent~~ in response to an authentication of **[[**~~said~~**]]** ~~at least~~ one of the client ~~device~~ devices.

3. (Currently amended) The network interface unit of claim 2, wherein **[[**~~said~~**]]** the configuration information ~~for each authenticated client device~~ comprises information received ~~on behalf of~~ in association with each of **[[**~~said~~**]]** the client devices upon an initial ~~authenticating~~ authentication of respective ones of [[said]] the client devices.

4. (Currently amended) The network interface unit of claim **[[**~~3~~**]]** 1, wherein ~~at least one of said client devices is a computer, and wherein said information received on behalf of a client device is received from one of said computers~~ the second client device is designated for authentication on behalf of the first client device and other incompatible client devices associated with the LAN.

5. (Cancelled).

6. (Currently amended) The network interface unit of claim **[[~~1~~]]** 2, wherein **[[~~said~~]]** the configuration information ~~for each~~ corresponding to the ~~authenticated~~ client devices comprises information related to connections to [[said]] the ~~at least~~ one or more non-secure ~~network~~ networks.

7. (Currently amended) The network interface unit of claim 6, wherein **[[~~said~~]]** the information related to **[[~~a~~]]** the connections to **[[~~said~~]]** the ~~at least~~ one or more non-secure ~~network~~ networks comprises information relating to ~~at least one~~ a dial-up connection.

8. (Currently amended) The network interface unit of claim 7, wherein **[[~~said~~]]** the information related to the ~~at least one~~ dial-up connection comprises information relating to ~~at least one~~ a customized dial-up connection, **[[~~said~~]]** the information relating to ~~each of said~~ the customized dial-up ~~connections~~ connection comprising a customized ~~dial-up~~ string of characters to control a ~~dial-up~~ modem connection to **[[~~said~~]]** the one or more non-secure ~~network~~ networks.

9. (Currently amended) The network interface unit of claim 6, wherein **[[~~said~~]]** the information related to the connections to **[[~~said~~]]** the ~~at least~~ one or more non-secure ~~network~~ networks comprises information relating to ~~at least one~~ a connection having a fixed IP address.

10. (Currently amended) The network interface unit of claim 6, wherein **[[~~said~~]]** the information related to the connections to **[[~~said~~]]** the ~~at least~~ one or more non-secure ~~network~~ networks comprises information relating to ~~at least one~~ a connection having a temporary IP address.

11. (Currently amended) The network interface unit of claim 10, further comprising a Dynamic Host Configuration Protocol (DHCP) ~~DHCP~~ server for providing **[[**~~said~~**]]** the temporary IP address.

12. (Currently amended) The network interface unit of claim **[[**~~10~~**]]** 6, further comprising a Dynamic Host Configuration Protocol (DHCP) ~~DHCP~~ client for obtaining a temporary IP address from **[[**~~said~~**]]** the at least one non-secure network and providing **[[**~~said~~**]]** the temporary IP address for use in [[said]] a connection.

13. (Currently amended) The network interface unit of claim 6, wherein **[[**~~said~~**]]** the information related to the connections to [[said]] the ~~at least~~ one or more non-secure ~~network~~ networks comprises information relating to ~~at least one~~ a point-to-point over Ethernet (PPPoE) connection.

14. (Currently amended) The network interface unit of claim 2, wherein **[[**~~said~~**]]** the memory comprises a removable memory module.

15. (Currently amended) The network interface unit of claim 14, wherein **[[**~~said~~**]]** the removable memory module stores ~~additional information comprising~~ web pages for presentation by **[[**~~said~~**]]** the graphical user interface ~~GUI~~ server.

16. (Currently amended) The network interface unit of claim 1, wherein **[[**~~said~~**]]** the means for authenticating the client devices comprises means for comparing a client **[[**~~ID~~**]]** identifier and password information received from **[[**~~a~~**]]** the client ~~device~~ devices with information stored at **[[**~~said~~**]]** the network interface unit.

17-20. (Cancelled).

Please add the following claims

21. (New) A method for communicating data packets over a non-secure network between client devices a secure virtual private network (VPN) node, comprising:

receiving a request from a first client device associated with a first local area network (LAN) to access the secure VPN node;

presenting an authentication menu via a graphical user interface on the first client device;

in response to receiving valid authentication information from the first client device, authenticating the first client device for access to the secure VPN node;

when a second client device associated with the first LAN is incompatible with the authentication menu, authenticating the second client device associated with the first LAN in response to the authentication of the first client device associated with the first LAN, the first client device being compatible with the authentication menu;

receiving a menu selection from the first client device corresponding to a connection profile associated with a first type of connection;

accessing the non-secure network using information associated with the selection; and

establishing a secure communication over the non-secure network between the first LAN and the secure VPN node.

22. (New) A method as defined in claim 21, wherein the first client device is designated for authentication on behalf of an incompatible client device, the first client device and the incompatible client device being associated with the same LAN.

23. (New) A tangible machine readable medium storing instructions that, when executed, cause a machine to:

receive a request from a first client device associated with a first local area network (LAN) to access a secure VPN node;

present an authentication menu via a graphical user interface to the first client device;

in response to receiving valid authentication information from the first client device, authenticate the first client device for access to the secure VPN node;

when a second client device associated with the first LAN is incompatible with the menu, authenticate the second client device of the first LAN in response to the authentication of the first client device of the first LAN;

receive a menu selection from the first client device corresponding to a connection profile associated with a first type of connection;

access a non-secure network using information associated with the selection; and

establish a secure connection over the non-secure network between the first LAN and the secure VPN.

24. (New) A tangible machine readable medium as defined in claim 23, wherein the first client device is designated for authentication on behalf of an incompatible client device associated with the first LAN.